UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,564	12/05/2003	Steve D. Huseth	(H0006281-0760)	8890

7590 10/06/2008

HONEYWELL INTERNATIONAL INC.
Law Dept. AB2
P.O. Box 2245
Morristown, NJ 07962-9806

EXAMINER	
NGUYEN, NAM V	

ART UNIT	PAPER NUMBER
2612	

MAIL DATE	DELIVERY MODE
10/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)	
Office Action Summary	10/728,564	HUSETH ET AL.	
	Examiner	**Art Unit**	
	Nam V. Nguyen	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-16,18-21,23-25,32-36 and 38-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 9-16, 18-21, 23-25, 32-36 and 38-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's Amendment which is filed June 20, 2008

An amendment to the claims 1, 7, 14, 26-32, 38-39 and 46-47 has been entered and made of record in the application of Huseth et al. for a "dual technology door entry person authentication."

Claims 26-31 are currently cancelled.

Claims 1-7, 9-16, 18-21, 23-25, 32-36 and 38-53 are now pending in the application.

Response to Arguments

In view of applicant's amendment to cancel the claims 26-31 to obviate the 35 U.S.C. §112 rejections, therefore, examiner has withdrawn the rejection under 35 U.S.C §112, second paragraph.

Applicant's amendments to the rejected claims are insufficient to distinguish the claimed invention from the cited prior arts or overcome the rejection of said claims under 35 U.S.C § 103(a) as discussed below. Applicant's amendment and argument with respect to the pending claims 1-7, 9-16, 18-21, 23-24, 32-36 and 38-53, filed June 20, 2008, have been fully considered but they are not persuasive for at least the following reasons.

Applicant's arguments with respect to claims 32-36 and 38-45, filed June 20, 2008 have been fully considered but are moot in view of the new ground(s) of rejection.

On page 21, fourth paragraph, Applicant's arguments with respect to the invention in Berardi does not teach or suggest that a processor is adapted to determine if said at least one RF signal is derived from said keyfob or said badge is not persuasive. The claims in a pending application should be given their broadest reasonable interpretation. In re Pearson, 181 USPQ 641 (CCPA 1974).

As defined by claims 1, 7, 14, 32, 38, and 46, Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The first embodiment of transponder 102 does not include a fingerprint reader (figure 2); this is interpreted as a badge. The second embodiment of transponder 102 includes a fingerprint reader (figure 9); this is interpreted as a keyfob. The figure 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. When the data is read from the transponder, a comparison is made to authorize financial access; this meets the limitation of determining if the received code is authentic and providing access upon authentication. If the data is from a badge, the authorization step compares account data (or the transponder ID), paragraph 59. If the data is from a keyfob the authorization step compares fingerprint data, paragraph 141. It is the examiner's position that in order to compare the received data from the figure 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. This meets the limitation of determining if the code is from a badge or keyfob. Clearly, Berardi et al. disclose the processor is adapted to determine if said at least one RF signal is derived from said keyfob or said badge.

Furthermore, the applicant argues that neither Berardi nor Fitzgibbon disclose a reader that is capable of receiving data from both a badge and a keyfob. Claims 1, 7, 14, 32, 38 and 46 do not set forth such limitations. The claims do set forth that the transceiver receives a signal from either a badge or a keyfob. Since the two types of devices are claimed in the alternative, only one type needs to be shown in the references. Furthermore, the RFID reader receives signal from transponder (114) with personal ID number recognized by the fob (102) to determine authorized access to complete transaction (page 14 paragraph 0137). The RFID reader also receives signal from another transponder (114) with biometric fingerprint signal to determine verification of the user's identity. Alternatively, the comparison may be made with a digitized fingerprint stored on a database maintained by the fob 102 transaction account provider system. The digitized fingerprint may be verified in much the same way as is described above with respect to the PIN (page 16 paragraph 0141; see Figure 9). Clearly, the RFID reader determines from the received signal either to compare the PIN or the digitized fingerprintBerardi actually shows both types (even though the applicant argues they are different embodiments) and therefore Berardi does meet the claimed limitation. In other words, the RFID reader (i.e. the transceiver) receives signal from one of the transponder and determine the received signal to validate the transaction.

Furthermore, Ritter discloses an external portable authorization-checking device (90) can access the user's identification and authorization data and reproduce these data optically. The external portable authorization-checking device (90) with a contactless interface using the same protocol and the same frequency as the identification module (40) (column 4 lines 13 to 22). the transmission of the identification parameters when entering or leaving the vehicle 35 can be triggered by the passengers or through the transceiver 32. The user ID data are read in the ID module 40 and transmit by means of appropriate communication protocols over the contactless interface to the transceivers 32 (column 6 lines 16 to 24; see Figure 4). Clearly the both devices using the same protocols in order to check whether the identification module really belongs to the user.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the same RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi et al. because using the same RF protocol would improve communication with plurality of access devices automatically in the access control system.

In an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. Fitzgibbon includes a processor (figure 4) in communication with the transmitters to process data received and make an authorization determination, see figure 8. Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The fingerprints and rolling codes are separately checked against databases for authenticity. See Figure 8.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi in view of Ritter because adding rolling code authentication increases security in the system.

The examiner maintains that the references cited and applied in the last office actions for the rejection of the claims are maintained in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 32-34 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berardi (2003/0167207) in view of Ritter (US# 7,084,736).

Referring to Claims 32-34 and 38, Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The first embodiment of transponder 102 does not include a fingerprint reader (figure 2); this is interpreted as a badge. The second embodiment of transponder 102 includes a fingerprint reader (figure 9); this is interpreted as a keyfob. The figure 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. When the data is read from the transponder, a comparison is made to authorize financial access; this meets the limitation of determining if the received code is authentic and providing access upon authentication. If the data is from a badge, the authorization step compares account data (or the transponder ID), paragraph 59. If the data is from a keyfob the authorization step compares fingerprint data, paragraph 141. It is the examiner's position that in order to compare the received data from the figure 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. This meets the limitation of determining if the code is from a badge or keyfob.

However, Berardi et al. did not explicitly disclose that the badge and the keyfob utilize the same RF protocol.

In the same field of endeavor of dual access communication system, Ritter teach that an identification data module 40 and an contactless interface 41 utilize the same RF protocol and the same frequency (column 4 lines 13 to 19; see Figures 1 to 3) in order to automatic checking and billing by readers and also identification data can be reproduced by the readers autonomously.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the same RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi et al. because using the same RF protocol would improve communication with plurality of access device autonomously in a access control system.

Claims 1-7, 9-16, 18-21, 23-25, 35-36, 39, 45-47 and 53, are rejected under 35 U.S.C. 103(a) as being unpatentable over Berardi et al. (2003/0167207) in view of Ritter (US# 7,084,736) and in further view of Fitzgibbon (2003/0210131).

Referring to Claims 1-6, Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The first embodiment of transponder 102 does not include a fingerprint reader (figure 2); this is interpreted as a badge. The second embodiment of transponder 102 includes a fingerprint reader (figure 9); this is interpreted as a keyfob. The figure 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. When the data is read from the transponder, a comparison is made to authorize financial access; this meets the limitation of determining if the received code is authentic and providing access upon authentication. If the data is from a badge, the authorization step compares account data (or the transponder ID), paragraph 59. If the data is from a keyfob the authorization step compares fingerprint data, paragraph 141. It is the examiner's position that in order to compare the received data from the figure 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. This meets the .limitation of determining if the code is from a badge or keyfob.

However, Berardi et al. did not explicitly disclose that the badge and the keyfob utilize the same RF protocol and wherein the authentication code from fingerprint keyfob comprises a digitized fingerprint signature and a rolling identifier.

In the same field of endeavor of dual access communication system, Ritter teach that an identification data module 40 and an contactless interface 41 utilize the same RF protocol and the same frequency (column 4 lines 13 to 19; see Figures 1 to 3) in order to automatic checking and billing by readers and also identification data can be reproduced by the readers autonomously.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the same RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi et al. because using the same RF protocol would improve communication with plurality of access device autonomously in a access control system.

In an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. Fitzgibbon includes a processor (figure 4) in communication with the transmitters to process data received and make an authorization determination, see figure 8. Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The fingerprints and rolling codes are separately checked against databases for authenticity. See Figure 8.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi in view of Ritter because adding rolling code authentication increases security in the system.

Referring to Claims 7, 9-16, 18-21, 23-25, 39 and 46-47, Berardi shows a method for providing access to a financial transaction, where the system includes two versions of the transponder 102. The first embodiment of transponder 102 does not include a fingerprint reader (figure 2); this is interpreted as a badge. The second embodiment of transponder 102 includes a fingerprint reader (figure 9); this is interpreted as a keyfob. The figure 9 transponder sends the fob ID (stored in memory 214) with the fingerprint so both can be authenticated. When the data is read from the transponder, a comparison is made to authorize financial access; this meets the limitation of determining if the received code is authentic and providing" access upon authentication. If the data is from a badge, the authorization step compares account data (or the transponder ID), paragraph 59. If the data is from a keyfob the authorization step compares fingerprint data, paragraph 141. It is the examiner's position that in order to compare the received data from the figure 9 transponder with stored fingerprint data, a decision inherently is made that the data received includes fingerprint data. This meets the limitation of determining if the code is from a badge or keyfob.

However, Berardi et al. did not explicitly disclose that the badge and the keyfob utilize the same RF protocol and wherein the authentication code from fingerprint keyfob comprises a digitized fingerprint signature and a rolling identifier and wherein the authentication code from the keyfob comprises first and second portions, wherein the first and second portions are different types of codes.

In the same field of endeavor of dual access communication system, Ritter teach that an identification data module 40 and an contactless interface 41 utilize the same RF protocol and the same frequency (column 4 lines 13 to 19; see Figures 1 to 3) and wherein the authentication code from the terminal 4 comprises identification data (i.e. first) and authorization data (i.e. second portions), wherein the first and second portions are different types of codes (column 5 lines 29 to 37; see Figures 1-3) in order to automatic checking and billing by readers and also identification data can be reproduced by the readers autonomously.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using the same RF protocol in the identification data module and an contactless interface for the authorization and checking device taught by Ritter in the RFID reader for interrogating the transponders of Berardi et al. because using the same RF protocol would improve communication with plurality of access device autonomously in a access control system.

In an analogous art, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. Fitzgibbon includes a processor (figure 4) in communication with the transmitters to process data received and make an authorization determination, see figure 8. Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The fingerprints and rolling codes are separately checked against databases for authenticity. See figure 8.

Therefore it would have been obvious to one of ordinary skill in the art at the time. of the invention to have used the fingerprint and rolling code processing of Fitzgibbon in the fingerprint entry transponder embodiment of Berardi in view Ritter because adding rolling code authentication increases security in the system.

Referring to Claims 35-36, Berardi et al. in view of Ritter and in further view of Fitzgibbon discloses the method of Claim 32, Fitzgibbon teaches an access security system where a transmitter can send codes to a garage door for access authorization. The portable transmitter (authorization module) can additionally include a fingerprint reader to send information regarding the user's fingerprint, also for authorization. Fitzgibbon includes a processor (figure 4) in communication with the transmitters to process data received and make an authorization determination, see figure 8. Fitzgibbon is cited for teaching that in this type of system, the use of rolling codes can improve the security of the system. The fingerprints and rolling codes are separately checked against databases for authenticity. See figure 8.

Referring to claims 45 and 53, Berardi et al. in view of Ritter disclose the method of Claims 38 and 46, however, Ritter did not explicitly disclose wherein said data is generated by said at least one of said plurality of authorization modules based on a shared and indexed mathematical function that prevents authorizing of said data, if said data is not authorized based on a particular sequence with respect to said shared and indexed mathematical function.

In the same field of endeavor of access control system, Fitzgibbon et al. disclose learning a rolling code and storing in an associated table via an address of the table, looking up in the code table is considered a shared and indexed mathematical function as claimed (see paragraph 0052; see Figure 5) in order to improve security in an access control system.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize using a rolling code and storing in an associated table taught by Fitzgibbon et al. in the RFID reader for interrogating the transponders for checking the authorization of users of Ritter because using rolling code and storing in an associated table would improve security in a communication of the access control authorization system.

Claims 40-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berardi (2003/0167207) in view of Ritter (US# 7,084,736) as applied to Claim 38, and in further view of Usui (US# 7,242,276).

Referring to claims 40-41, Berardi in view of Ritter disclose the method of Claim 38, however, Ritter did not explicitly disclose that wherein said access device comprises a door lock and wherein said door lock comprises a stand alone push button lock that utilizes an authentication code to activate said stand alone push button lock, wherein said authentication code is changeable utilizing said processor.

In the same field of endeavor of access control system, Usui disclose a door lock system (1) (column 2 lines 16 to 26; see Figure 1); and wherein said door lock (1) comprises a stand alone push button lock that utilizes an authentication code to activate said stand alone push button lock, wherein said authentication code is changeable utilizing said control unit 30 (i.e. processor) (column 2 lines 27 to 62; see Figures 1-3) in order to improve security of a doorway locking system.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to recognize applying the door lock system with authentication code to activate the lock taught by Usui in the RFID reader for interrogating the transponders for checking the authorization of users of Ritter because using authentication code to activate the door lock would improve a plurality of utility of the access control system.

Referring to claims 42-43, Berardi in view of Ritter disclose the method of Claim 38, and Usui discloses a fingerprint keyfob reader (column 2 lines 39 to 46; see Figures 2 and 3).

Referring to claim 44, Berardi in view of Ritter disclose the method of Claim 38, and Usui discloses a fingerprint keyfob reader (column 2 lines 39 to 46; see Figures 2 and 3), it would be obvious to replace the finger print reader with a magnetic strip reader because the magnetic stripe reader is conventional reader.

Claims 48-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berardi (2003/0167207) in view of Ritter (US# 7,084,736) and Fitzgibbon (2003/0210131) as applied to Claim 46, and in further view of Usui (US# 7,242,276).

Referring to claims 48-52, Berardi in view of Ritter and Fitzgibbon disclose the access control method of claim 46, the claims 48-52 same in that the claims 40-44 already addressed above therefore claims 48-52 are also rejected for the same obvious reasons given with respect to claim 40-43.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 571-272-3061. The examiner can normally be reached on Mon-Fri, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman can be reached on 571- 272-3059. The fax phone numbers for the organization where this application or proceeding is assigned are 571-273-8300 for regular communications.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Brian A Zimmerman/
Supervisory Patent Examiner, Art Unit 2612